Hilbert’s Tenth Problem for Fixed $d$ and $n$
by William Gasarch

1 Hilbert’s Tenth Problem

(Everything in this document is known.)

In 1900 Hilbert proposed 23 problems for mathematicians to work on over the next 100 years (or longer). The 10th problem, stated in modern terms, is

Find an algorithm that will, given $p \in \mathbb{Z}[x_1, \ldots, x_n]$, determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.

Hilbert probably thought this would inspire much deep number theory. And it did inspire some. However, through the efforts of Davis, Putnam, Robinson [1] and Matiyasevich [4] (see also the book by Matiyasevich [5]) it was shown that there is no such algorithm. That is, they showed that there is a $d, n$ such that the problem of, given $p \in \mathbb{Z}[x_1, \ldots, x_n]$ of degree $d$, does it have a solution in $\mathbb{Z}$, is undecidable.

This raises the obvious question of what happens for particular numbers of variables $n$ and degree $d$. I thought that surely there must be a grid on the web where the $d$-$n$-th entry is

- D if the problem for degree $\leq d$, and $\leq n$ variables is Decidable.
- U if the problem for degree $\leq d$, and $\leq n$ variables is Undecidable.
- ? if the status of the problem for degree $\leq d$, and $\leq n$ variables is unknown.

Why was there no such grid? I speculate

1. Logicians worked on proving particular $(d,n)$ are undecidable. They sought solutions in $\mathbb{N}$. By contrast number theorists worked on proving particular $(d,n)$ decidable. They sought solutions in $\mathbb{Z}$. Hence a grid would need to reconcile these two related problems.

2. Logicians and number theorists didn’t talk to each other. Websites and books on Hilbert’s Tenth problem do not mention any solvable cases of it.

3. There is a real dearth of positive results, so a grid would not be that interesting. Note that we do not even know if the following is decidable: given $k \in \mathbb{Z}$ does there exists $x, y, z \in \mathbb{Z}$ such that
\[ x^3 + y^3 + z^3 = k. \]

4. The undecidable results often involve rather large values of \( d \), so the grid would be hard to draw.

Hence I gave up on finding or creating a grid, and instead collected up all the results I could find. If I missed any then please let me know.

**Notation 1.1**

1. \( \text{H10Z}(d, n) \) is the problem where the degree is \( \leq d \), the number of variables is \( \leq n \), and we seek a solution in \( \mathbb{Z} \).

2. \( \text{H10N}(d, n) \) is the problem where the degree is \( \leq d \), the number of variables is \( \leq n \), and we seek a solution in \( \mathbb{N} \).

3. \( \text{H10Z}(d, n) = D \) means that there is an algorithm to decide \( \text{H10Z} \)

4. \( \text{H10Z}(d, n) = U \) means that there is no algorithm to decide \( \text{H10Z} \)

5. Similarly for \( \text{H10N}(d, n) \) equal to \( D \) or \( U \).

**Lemma 1.2**

1. For every \( x \in \mathbb{N} \), there exists \( y_1, y_2, y_3, y_4 \in \mathbb{N} \) such that
   \[ x = y_1^2 + y_2^2 + y_3^2 + y_4^2. \]

2. For every \( x \in \mathbb{N} \) where \( x \) is not of the form \( 4^a(8b + 7) \), there exists \( y_1, y_2, y_3 \in \mathbb{N} \) such that
   \[ x = y_1^2 + y_2^2 + y_3^2. \]

3. For every \( x \in \mathbb{N} \) where \( x \equiv 1 \pmod{4} \), there exists \( y_1, y_2 \equiv 0 \pmod{2} \) and \( y_3 \equiv 1 \pmod{2} \), such that
   \[ x = y_1^2 + y_2^2 + y_3^2. \]

4. For every \( x \in \mathbb{N} \), there exists \( y_1, y_2, y_3 \in \mathbb{N} \) such that
   \[ x = y_1^2 + y_2^2 + y_3^2 + y_4. \]
Proof:
1) This is Lagrange’s 4-square theorem.
2) This is Legendre’s 3-square theorem. It is sometimes called the Gauss-Legendre Theorem.
3) Since \( x \equiv 1 \pmod{4} \), \( x \) satisfies the hypothesis of part 2. Hence there exists \( y_1, y_2, y_3 \) such that

\[
x = y_1^2 + y_2^2 + y_3^2.
\]

Take this equation mod 4.

\[
1 \equiv y_1^2 + y_2^2 + y_3^2 \pmod{4}.
\]

It is easy to see that the only parities of \( y_1, y_2, y_3 \) that work are for two of them to be even and one of them to be odd.
4) By part 3, for every \( x \) there exists \( y_1, y_2, y_3 \) such that

\[
4x + 1 = (2y_1)^2 + (2y_2)^2 + (2y_3 + 1)^2.
\]

\[
4x + 1 = 4y_1^2 + 4y_2^2 + 4y_3^2 + 4y_3 + 1.
\]

\[
x = y_1^2 + y_2^2 + y_3^2 + y_3.
\]

Theorem 1.3

1. If \( H_{10Z}(2d, 4n) = D \), then \( H_{10N}(d, n) = D \).
2. If \( H_{10N}(d, n) = U \), then \( H_{10Z}(2d, 4n) = U \). This is the contrapositive of part 1.
3. If \( H_{10Z}(2d, 3n) = D \), then \( H_{10N}(d, n) = D \).
4. If \( H_{10N}(d, n) = U \), then \( H_{10Z}(2d, 3n) = U \). This is the contrapositive of part 3.
5. If \( H_{10Z}(f(d, n), 2n + 2) = D \), then \( H_{10N}(d, n) = D \) where

\[
f(d, n) = \max\{2d, (2n + 3)2^n\}.
\]

6. If \( H_{10N}(d, n) = U \), then \( H_{10Z}(f(d, n), 2n + 2) = U \). This is the contrapositive of part 5.
Proof:

1) Assume $H_{10}\mathbb{Z}(2d, 4n) = D$. We show that $H_{10}\mathbb{N}(d, n) = D$.

Let $p \in \mathbb{Z}[x_1, \ldots, x_n]$. We want to know if there is a solution in $\mathbb{N}$.

Let $q$ be the polynomial of degree $2d$ with $4n$ variables that you get if you replace each $x_i$ with $y_{i1}^2 + y_{i2}^2 + y_{i3}^2 + y_{i4}^2$ where $y_{i1}, y_{i2}, y_{i3}, y_{i4}$ are 4 new variables. By Lemma 1.2.1 and the fact that for all $w, x, y, z \in \mathbb{Z}$, $w^2 + x^2 + y^2 + z^2 \geq 0$, we have:

$p$ has a solution in $\mathbb{N}$ iff $q$ has a solution in $\mathbb{Z}$.

Use that $H_{10}\mathbb{Z}(2d, 4n) = D$ to determine if $q$ has a solution. Hence $H_{10}\mathbb{N}(d, n) = D$.

3) Let $p \in \mathbb{Z}[x_1, \ldots, x_n]$. We want to know if there is a solution in $\mathbb{N}$.

Let $q$ be the polynomial of degree $2d$ with $3n$ variables that you get if you replace each $x_i$ with $y_{i1}^2 + y_{i2}^2 + y_{i3}^2 + y_{i3}$ where $y_{i1}, y_{i2}, y_{i3}$ are 3 new variables. By Lemma 1.2.3 and the fact that for all $w, x, y \in \mathbb{N}$, $w^2 + x^2 + y^2 + y \geq 0$, we have:

$p$ has a solution in $\mathbb{N}$ iff $q$ has a solution in $\mathbb{Z}$.

Use that $H_{10}\mathbb{Z}(2d, 3n) = D$ to determine if $q$ has a solution. Hence $H_{10}\mathbb{N}(d, n) = D$.

5) This was proven by Zhi-Wei Sun [7]. We sketch his proof.

Def 1.4 Let $F_i$ be the $i$th Fibonacci number. Let $k \in \mathbb{N}$. Then define $H_k \in \mathbb{Z}[y_1, \ldots, y_k, z_1, z_2, x]$ by

$$H_k(y_1, \ldots, y_k, z_1, z_2, w) = F_0 z_1^0 (z_1 w + z_2)^{2^k} + F_1 z_1 (z_1 w + z_2)^{2^k-1} + \cdots + F_{2^k-1} z_1^{2^k-1} (z_1 w + z_2) + F_{2^k} z_1^{2^k}.$$ 

Note that $H_k$ has $k + 3$ variables and is of degree $2^k$.

He proves that, for all polynomials $Q \in \mathbb{Z}[x_1, \ldots, x_n]$, $Q(x_1, \ldots, x_n)$ has a solution with all $x_i \in \mathbb{N}$ iff the following polynomial in $x_1, \ldots, x_n, y_0, \ldots, y_{n+1}$ has a solution with all of the variables in $\mathbb{Z}$:

$$Q(x_1, \ldots, x_n)^2 + H_n((4x_1+2)y_1^2+1, \ldots, (4x_{n-1}+2)y_{n-1}^2+1, (4(x_n+1)y_1^2 \cdots y_{n-1}^2 - 2)(2y_n-1)^2(3y_{n+1}-1)^2 + 1, 1, 0, y_0).$$

Note that the second polynomial has only $2n + 2$ variables.

Assume that $Q$ has degree $d$. The degree of $Q^2$ is $2d$. The degree of the term

$$(4(x_n+1)y_1^2 \cdots y_{n-1}^2 - 2)(2y_n-1)^2(3y_{n+1}-1)^2 + 1$$

is $2d + 1$. Therefore $Q(x_1, \ldots, x_n)$ has a solution.
is $2n + 3$. The degree of $H_n$ is $2^n$. Hence the degree of the second polynomial is
\[ \max\{2d, (2n+3)2^n\}. \]

\[ \]

**Theorem 1.5**

1. If $H_{10}^\mathbb{N}(d, n) = D$ then $H_{10}^\mathbb{Z}(d, n) = D$.

2. If $H_{10}^\mathbb{Z}(d, n) = U$ then $H_{10}^\mathbb{N}(d, n) = U$. This is the contrapositive of part 1.

**Proof:** Let $p \in \mathbb{Z}[x_1, \ldots, x_n]$. We want to know if there is a solution in $\mathbb{Z}$. For each \( \vec{b} = (b_1, \ldots, b_n) \in \{0, 1\}^n \) let $q_{\vec{b}}(x_1, \ldots, x_n)$ be formed as follows: for every $i$ where $b_i = 1$, replace $x_i$ with $-x_i$. It is easy to see that
\[ p \text{ has a solution in } \mathbb{Z} \text{ iff there exists } \vec{b} \text{ such that } q_{\vec{b}} \text{ has a solution in } \mathbb{N}. \] The result follows.

In the next section we summarize what is known about $H_{10}^\mathbb{N}(d, n)$. 

5
2 When Is $H_10^N(d, n) = U$? $H_10^Z(d, n) = U$?

The following theorem has many $H_10^N(a, b) = U$, all due to Jones [3]. From those we use Theorem 1.3 to obtain several $H_10^Z(c, d) = U$ results.

**Theorem 2.1**

1. $H_10^N(4, 58) = U$ hence $H_10^Z(8, 174) = U$ and $H_10^Z(119 \times 2^{58}, 118) = U$.
2. $H_10^N(8, 38) = U$ hence $H_10^Z(16, 114) = U$ and $H_10^Z(79 \times 2^{38}, 78) = U$.
3. $H_10^N(12, 32) = U$ hence $H_10^Z(24, 96) = U$ and $H_10^Z(67 \times 2^{32}, 66) = U$.
5. $H_10^N(20, 28) = U$ hence $H_10^Z(40, 84) = U$ and $H_10^Z(59 \times 2^{28}, 58) = U$.
6. $H_10^N(24, 26) = U$ hence $H_10^Z(48, 78) = U$ and $H_10^Z(55 \times 2^{26}, 54) = U$.
8. $H_10^N(36, 24) = U$ hence $H_10^Z(72, 72) = U$ and $H_10^Z(51 \times 2^{24}, 50) = U$.
11. $H_10^N(200000, 14) = U$ hence $H_10^Z(400000, 42) = U$ and $H_10^Z(31 \times 2^{14}, 30) = U$.
13. $H_10^N(1.3 \times 10^{44}, 12) = U$ hence $H_10^Z(2.6 \times 10^{44}, 36) = U$ and $H_10^Z(2.6 \times 2^{44}, 26) = U$.
14. $H_10^N(4.6 \times 10^{44}, 11) = U$ hence $H_10^Z(9.2 \times 10^{44}, 33) = U$ and $H_10^Z(9.2 \times 2^{44}, 24) = U$.
15. $H_10^N(8.6 \times 10^{44}, 10) = U$ hence $H_10^Z(17.2 \times 10^{44}, 30) = U$ and $H_10^Z(17.2 \times 2^{44}, 22) = U$.
16. $H_10^N(1.6 \times 10^{45}, 9) = U$ hence $H_10^Z(3.2 \times 10^{45}, 27) = U$ and $H_10^Z(3.2 \times 2^{45}, 20) = U$. 


3 When is $H_{10}(d, n) = D$? When is $H_{10}(d, n) = D$?

**Theorem 3.1**

1. For all $d$, $H_{10}(d, 1) = D$. This is elementary.
2. For all $d$, $H_{10}(d, 1) = D$. This is elementary.
3. For all $n$, $H_{10}(1, n) = D$. This is elementary.
4. For all $n$, $H_{10}(1, n) = D$. This is elementary.
5. $H_{10}(2, 2) = D$ and $H_{10}(2, 2) = D$. I have not found a paper that says this explicitly, however, [https://www.alpertron.com.ar/QUAD.HTM](https://www.alpertron.com.ar/QUAD.HTM) seems to imply it.
6. For all $n$, $H_{10}(2, n) = D$. This is a sophisticated theorem due to Siegel [6]. See also Grunewald and Seigel [2].

The smallest $(a, b)$ such that $H_{10}(a, b)$ is unknown seems to be $(3, 2)$.

7. The smallest $(a, b)$ such that $H_{10}(a, b)$ is unknown seems to be $(3, 2)$.

4 Acknowledgement

We thank David Marcus for proofreading and commentary.

References


